The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

05/22/2013

SUBJECT:

Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can be exploited if a user visits, or is redirected to a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEM AFFECTED:

Google Chrome for Windows, Mac and Linux versions prior to 27.0.1453.93

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Google Chrome, Details of these vulnerabilities are as follows:

A use-after-free issue in SVG. [CVE-2013-2837]

An out-of-bounds read issue in v8. [CVE-2013-2838]

A security vulnerability exists due to bad cast in clipboard handling. [CVE-2013-2839]

A use-after-free issue in media loader. [CVE-2013-2840]
A use-after-free issue in pepper resource handling. [CVE-2013-2841]
A use-after-free issue in widget handling. [CVE-2013-2842]